Security Advisory Report - OBSO-2206-01

Impact of critical Expat vulnerabilities on Atos Unify OpenScape Xpert (CVE-2022-23990 / CVE-2022-23852)

Release Date:	2022-02-10 10:11:56
Last Update:	2022-06-29 10:44:53
Version:	1.0

Summary

PUBLIC - FOR EXTERNAL USE (TLP: WHITE)

Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

2 Critical vulnerabilities (CVE-2022-23990, CVE-2022-23852) have been identified for the Expat XML parser before Expat version 2.4.4. They may impact the security of Atos Unify Xpert MLC V6 and V7. Both vulnerabilities are integer overflow vulnerabilities that may be triggered under certain conditions. If the condition may be triggered by user supplied input, the vulnerabilities may have an impact on the security of the product. The impact currently is not clear and there are no public exploits available for the vulnerabilities. As a precaution measure, we issue this security advisory to inform about available mitigation measures and planned updates.

For OpenScape Xpert MLC the severity of the vulnerability is rated high to medium.

The security advisory will initially be shared to registered subscribers via obso@atos.net and as a Knowledge Base article KB000103030 within the Atos Unify ServiceNow support portal. You may share this security advisory to Atos Unify customers and partners put not publish it on a publicly available website.

Details

Vulnerability details:

CVE-2022-23852
Expat (aka libexpat) before 2.4.4 has a signed integer overflow in XML_GetBuffer, for configurations with a nonzero XML_CONTEXT_BYTES.
CVSS3.1 Base score: 9.8
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2022-23990
CVSS3.1 Base score: 9.8
Expat (aka libexpat) before 2.4.4 has an integer overflow in the doProlog function.
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Severity rating:

While severity rating of the specific vulnerability is rated critical with a CVSS3.1 base score of 9.8 considering the temporal and environmental score the severity rating of the vulnerabilities in the context of OpenScape Xpert is considered high to medium.

The temporal and environment parameters of the CVSS3.1 the temporal score is 8.0 (high) the environmental score is 6.1 (medium):

- There is currently no proven exploit
- There is workaround/mitigation measure available (implement TLS on the SIP interface between OpenScape Xpert MLC and the SIP-Server (PBX))
- The impact on the product is currently unknown
- OpenScape Xpert is running in a secured network (Modified Attack Vector = Adjacent)
- Modified Attack Complexity is High (an attacker would have to investigate the product offline, get access to the network)

External ratings:

- CVE-2022-23990: CERT-Bund rates the vulnerability with medium risk (3//5)
- CVE-2022-23852: CERT-Bund rates the vulnerability with low risk (2//5)

Affected Products

Products confirmed affected

Atos Unify OpenScape Xpert MLC V6 and V7 before V7 R4.0.0

Products confirmed not affected

Atos Unify OpenScape Xpert MLC V7 R4.0.0 and higher
Atos Unify OpenScape Xpert Clients V6 and V7
Atos Unify OpenScape Xpert System Manager V6 and V7

Recommended Actions

In order to reduce the potential impact of the vulnerabilities it is recommended to use TLS on the SIP interface between OpenScape Xpert MLC and and the SIP-Server (PBX)).
The implementation of TLS prevents that an unauthenticated attacker is able to exploit the issue.

Update to version V7 R4.0.0 and higher
It is recommended to update to version V7 R4.1.0 (includes Expat V2.4.8 fixing additional vulnerabilities)

References

External References

- https://nvd.nist.gov/vuln/detail/CVE-2022-23852
- https://nvd.nist.gov/vuln/detail/CVE-2022-23990
- https://cwe.mitre.org/data/definitions/190.html
- https://www.heise.de/news/XML-Parser-Expat-ermoeglicht-Angreifern-Einschleusen-von-Schadcode-6341560.html
- https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/2022/01/warnmeldung_cb-k22-0114_update_1.html?nn=129588
- https://www.cert-bund.de/advisoryshort/CB-K22-0091

Version Change History

Version	Date	Description
0.1	14.02.2022	- Initial draft, not publicly disclosed on website. See KB000103030
1.0	29.06.2022	- Initial release

Advisory: OBSO-2206-01, status: ready for review
Security Advisories are released as part of Atos Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer

OpenScape Baseline Security Office
obso@atos.net

Otto-Hahn-Ring 6
D-81739 München
www.unify.com

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a

result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.
Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG.

All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.